Figure 1

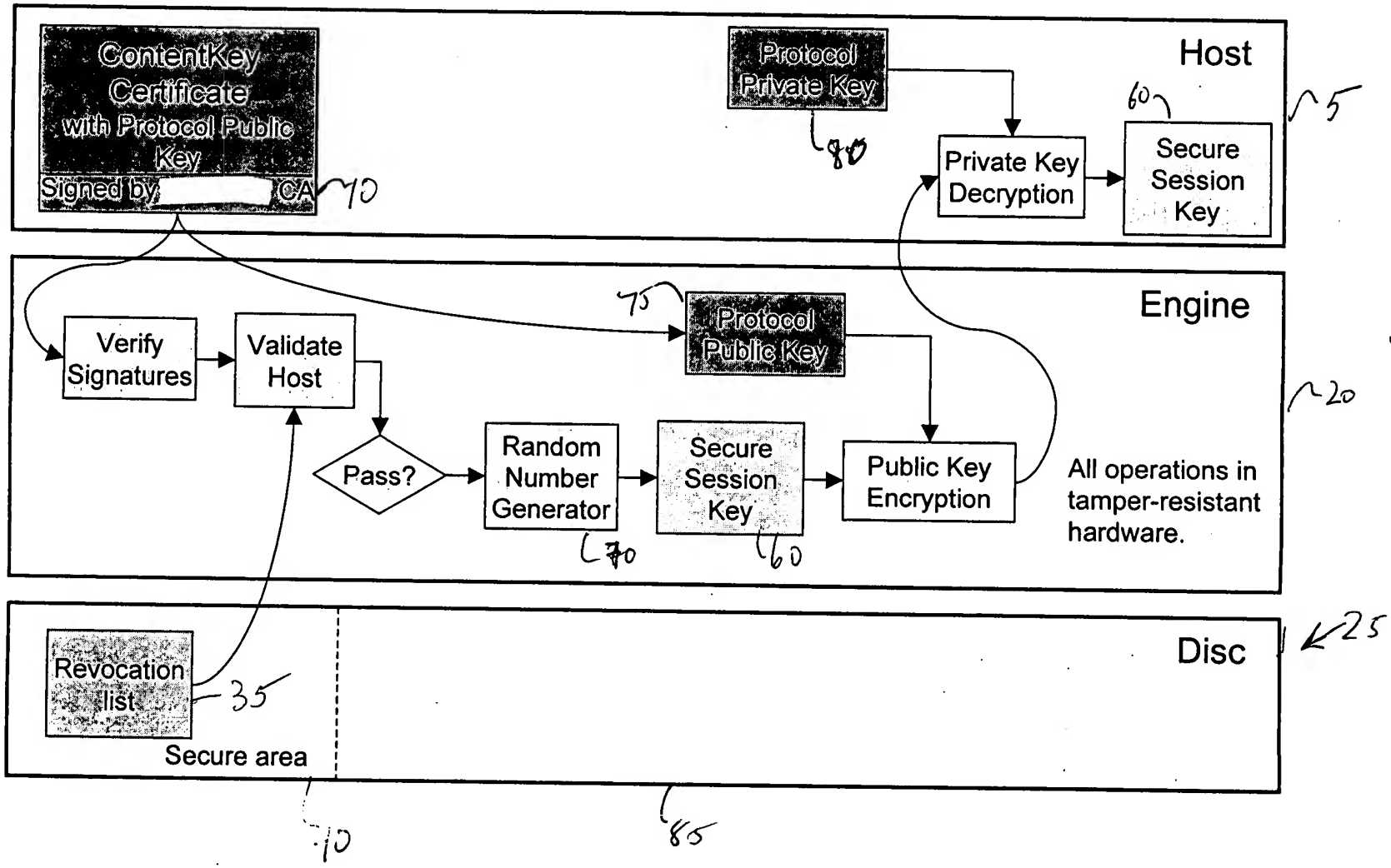

Host
ContentKey Certificate with Protocol Public Key
Signed by CA
10
Protocol Private Key
80
Private Key Decryption
60
Secure Session Key
5
Engine
75
Protocol Public Key
Verify Signatures
Validate Host
Pass?
Random Number Generator
70
Secure Session Key
60
Public Key Encryption
All operations in tamper-resistant hardware.
20
Disc
25
Revocation list
35
Secure area
10
85

Figure 2

CK Implementation on HDD Devices

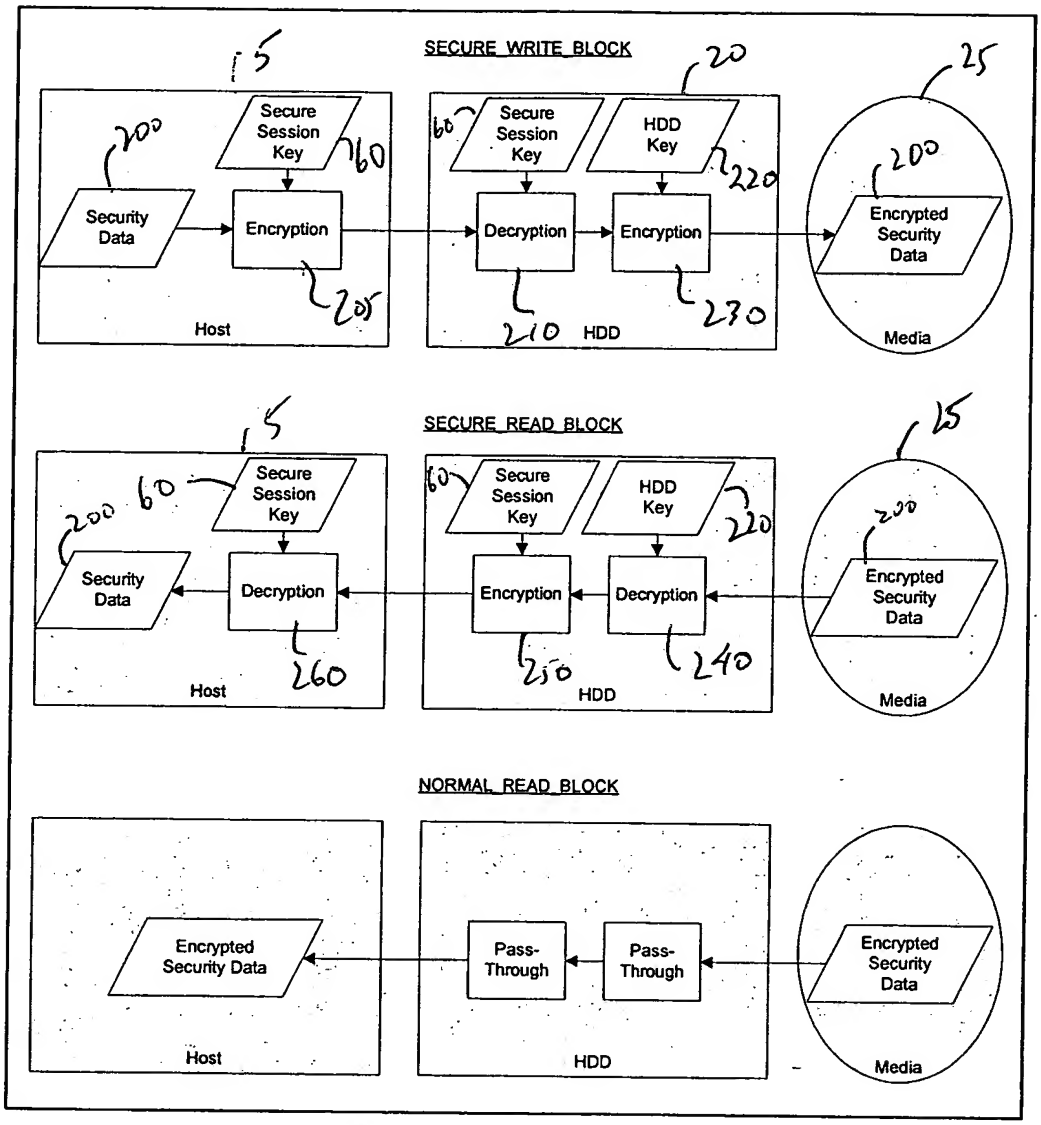


Figure 3

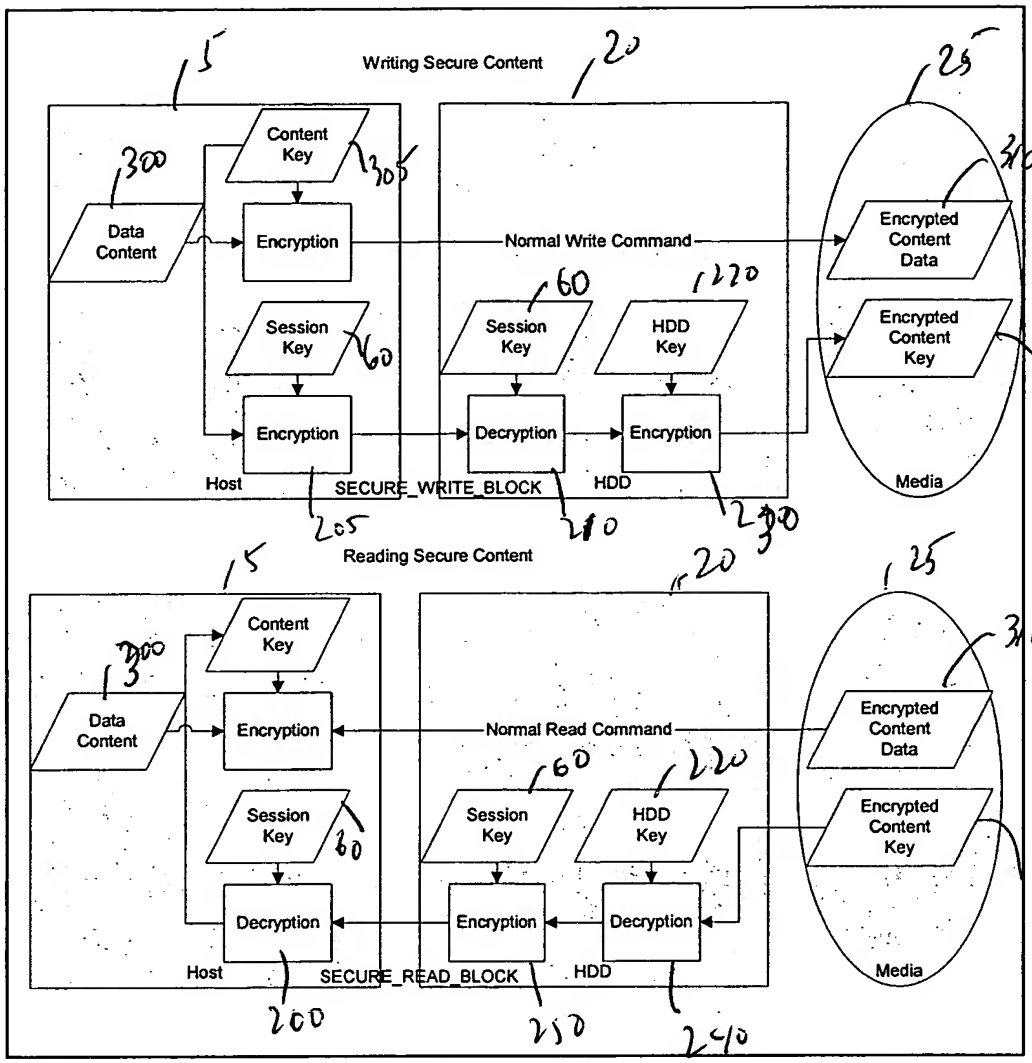

Writing Secure Content
15
20
25
Content Key
305
300
Data Content
Encryption
Normal Write Command
Encrypted Content Data
310
Session Key
60
Session Key
60
HDD Key
220
Encrypted Content Key
307
Encryption
Decryption
Encryption
Host
SECURE_WRITE_BLOCK
HDD
Media
205
210
230
Reading Secure Content
15
20
25
Content Key
300
Data Content
Encryption
Normal Read Command
Encrypted Content Data
310
Session Key
60
Session Key
60
HDD Key
220
Encrypted Content Key
307
Decryption
Encryption
Decryption
Host
SECURE_READ_BLOCK
HDD
Media
200
250
240

Figure 4

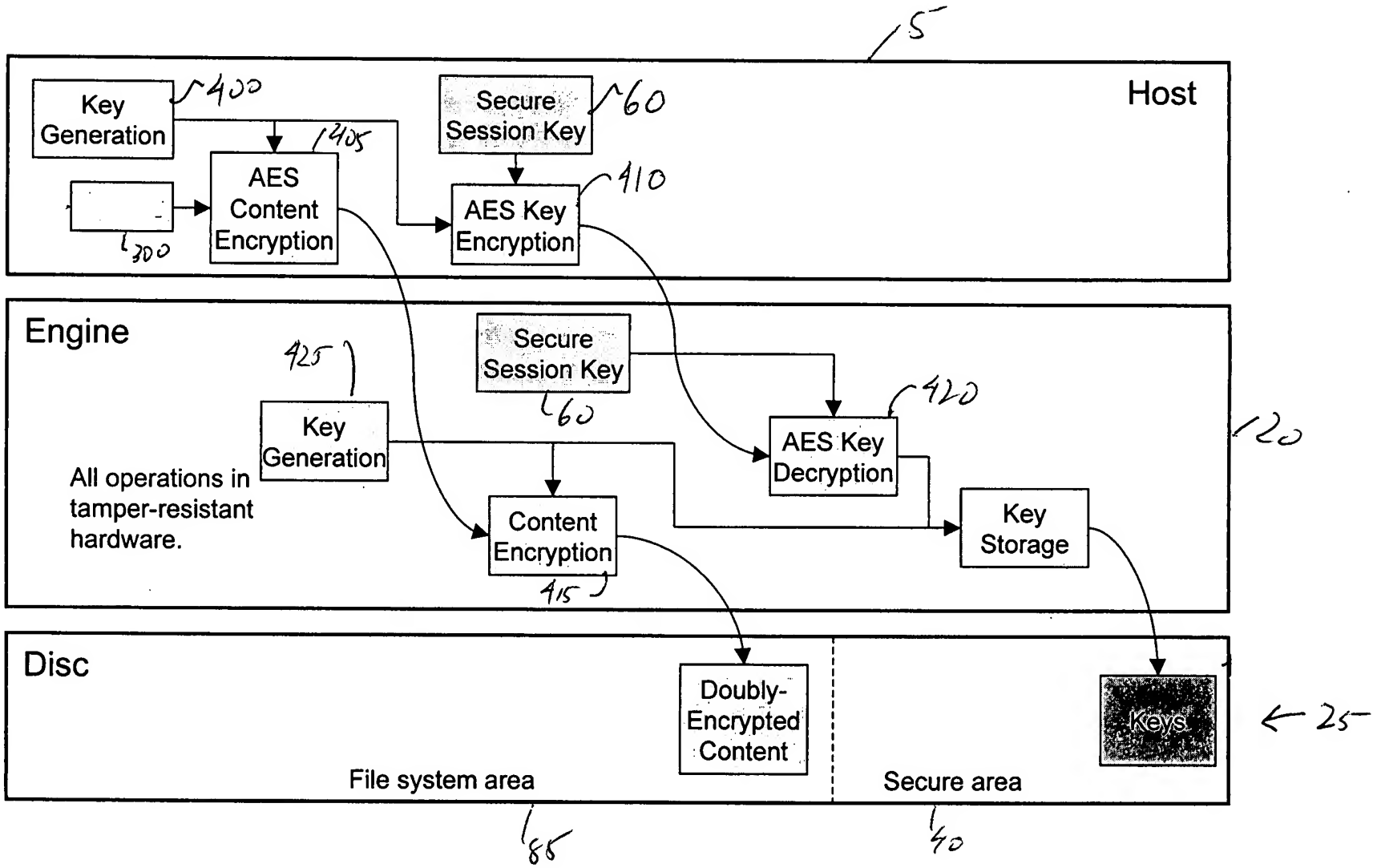

5
Host
Key Generation
400
405
Secure Session Key
60
AES Content Encryption
410
AES Key Encryption
300
Engine
425
Secure Session Key
60
Key Generation
420
AES Key Decryption
All operations in tamper-resistant hardware.
Content Encryption
415
Key Storage
20
Disc
Doubly-Encrypted Content
Keys
25
File system area
Secure area
85
40

Figure 5

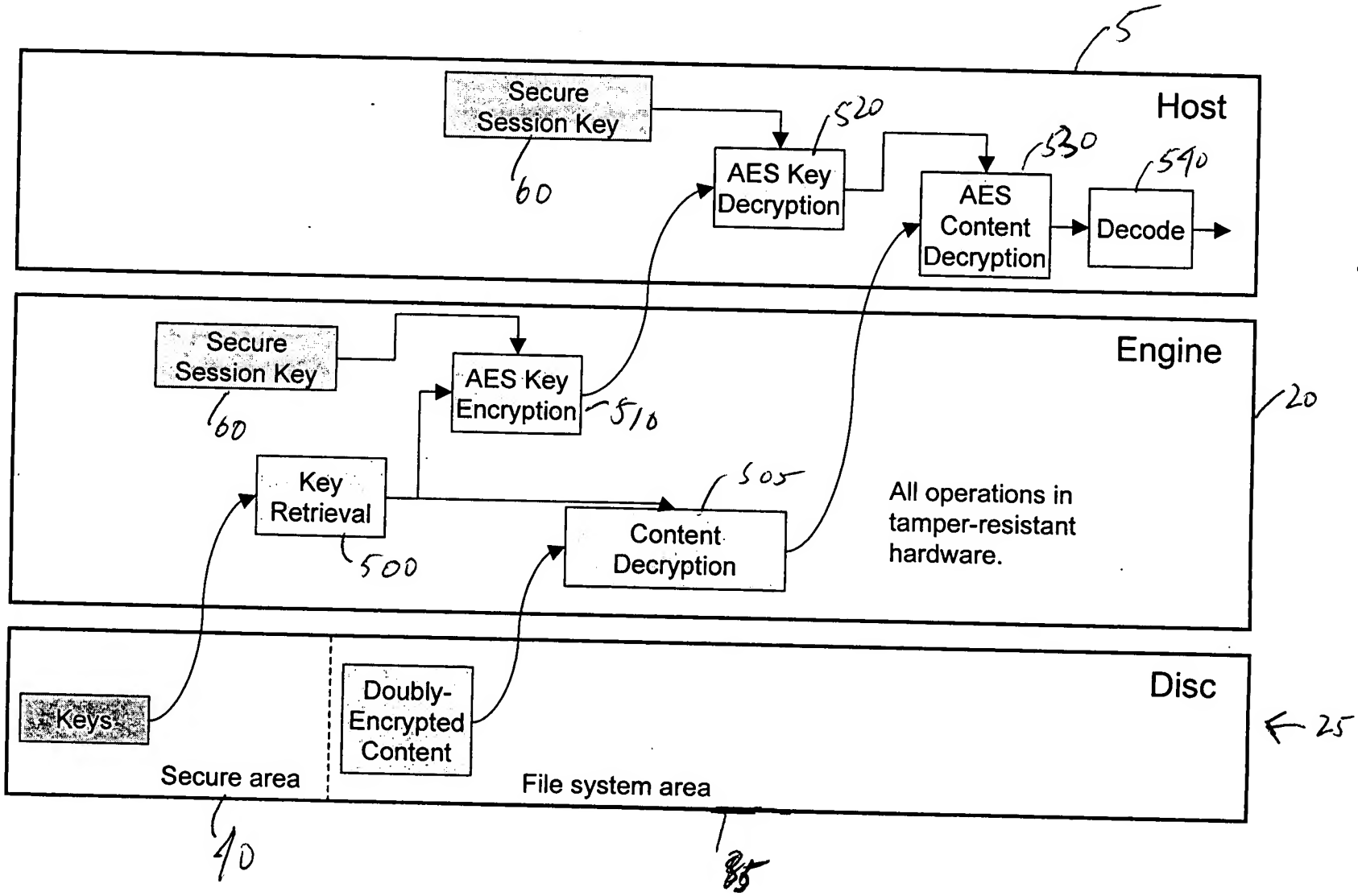
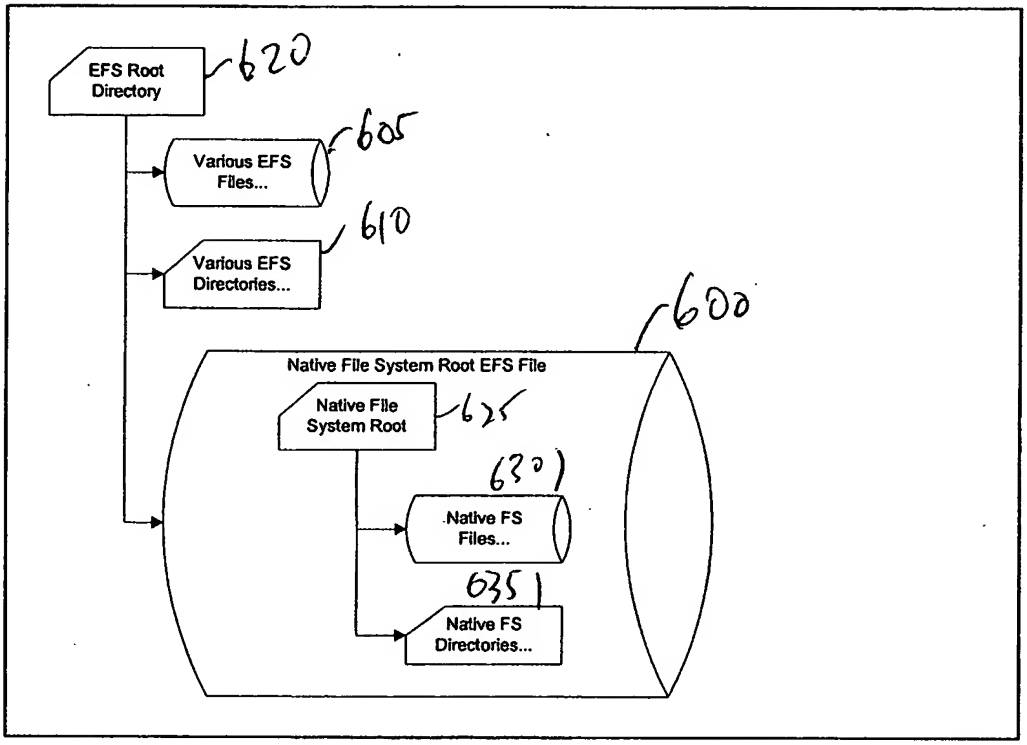

5
Host
Secure Session Key
60
520
AES Key Decryption
530
AES Content Decryption
540
Decode
Engine
20
Secure Session Key
60
AES Key Encryption
510
Key Retrieval
500
505
Content Decryption
All operations in tamper-resistant hardware.
Disc
25
Keys
Secure area
40
Doubly-Encrypted Content
File system area
85

Figure 6


EFS Root Directory
620
Various EFS Files...
605
Various EFS Directories...
610
600
Native File System Root EFS File
Native File System Root
625
630
Native FS Files...
635
Native FS Directories...